Digital Devices Acceptable Use Policy

Prepared by	Assistant Principal K-12 – Steve Tidey
Number of pages	9
Date reviewed	November 2023
Monitored by	Principal
Review by	Executive
Date for review	January 2025 or where changes are required due to legislative requirements
Status	Active
Updated	November 2023

VISION

The College's vision is that we might be a Christian community which seeks to nurture and train young people to grow up into Christ.

CONTEXT

Belmont Christian College is committed to fostering a community that encourages and exhibits relationships, attitudes and behaviours that are based on biblical beliefs, practices and values. The College seeks to create a caring environment where Christian values inspire and affirm the highest standards of ethical conduct in relation to the care, support, and wellbeing of the students entrusted to it. The College seeks to cultivate an environment that contributes to the spiritual, personal, social and physical development of the child.

The College Code of Conduct for all members of the community reflects respect; that each person will act kindly and courteously, and with respect for others; that each person will not force themselves or anything that they own physically, verbally or emotionally on others; and that each person has the privilege, if done respectfully, to ask questions of another. This code can be summarised by the key words: Respect, Responsibility, Integrity, Citizenship, Compassion, Gratitude.

PURPOSE

This policy and its associated policies (see the suite of Safe & Supportive Environment Policies, Online Teaching & Learning Policy, Communication Policy) outline the rights and responsibilities of members of the College community in regard to device use, network access and conduct that affect the wellbeing and safety of students. They also protect and enhance the College's unique culture anchored in biblical truth that informs ethical and professional decisions and actions. This is a culture of respect: respect for one another as people created in the image of God and care for the physical environment and individual property. The purpose of this policy is to foster a safe and supportive environment where students' attitudes and behaviours are consistent with the culture of the College as expressed in the Code of Conduct.

POLICY STATEMENT

The objectives of the policy can best be fulfilled within the context of an active community. The College recognises the interdependent relationship of four aspects of our community: the student, the home, the teacher and the College. Fellowship will be maintained and strengthened through all parties having a common belief and a commitment to communicating well with each other. In short, to know what the guidelines are, discuss the issues and come to a conclusion based on what is best for the child.

All students who are enrolled at Belmont Christian College (BCC) are to be kept safe from abuse, harm and mistreatment, are encouraged to maintain respectful relationships, and be wise and responsible users of technology in order to thoughtfully integrate faith and life. We want to foster our students' ability to live as young people who faithfully translate the Gospel into the culture around them.

This policy is based on the principles of mutual responsibility and respect of all parties involved in the use of digital devices which includes mobile phones and smartwatches. It requires accountability on the part of the user for their actions. It is designed to assist in managing the safe and responsible use of mobile digital devices by students and involves parents/carers as partners in assisting their children in the proper use of said devices. It is underpinned by Biblical principles and an overall requirement for students to exercise care, to use their devices in a considerate manner and to be aware of situations in which others could be affected by their actions. It makes clear that the privilege to have a mobile digital device such as a tablet, a mobile phone/smartwatch at school may be withdrawn if a student fails in their duty to behave responsibly and in accordance with the College's requirements.

DUTY OF CARE:

All College community members have a duty to take reasonable care for the safety and welfare of students in their care. That duty is to consider and take all reasonable action to protect students from known hazards or risk of harm that can be reasonably predicted. The standard of care that is required of a College community member must take into consideration various factors such as a student's age, maturity and ability.

This duty of care owed to students by all College community members applies during all activities and functions conducted or arranged by the College where a student is in the care of a College community member. The risk associated with any activity needs to be assessed and managed by College community members before the activity is undertaken. A single serious failure to exercise appropriate duty of care, or persistent repeated failures, may constitute neglect or negligence according to the law if actual harm is caused, or if there is the potential to cause significant harm to a student.

RATIONALE

At Belmont Christian College we want our students to become good "digital citizens" able to confidently locate and use information which is accurate, relevant, authoritative, comprehensive and balanced. We also desire that they should use technology thoughtfully, ethically and respectfully and aware of the "digital footprint" they are leaving behind. All Secondary students are equipped with a College provided email address to enhance the communication between staff and other students.

DEVICE REQUIREMENTS

All students in Years 5 – 10 use a College approved Chromebook. These devices conform to a set of minimum requirements as set out by the College and must be purchased via the approved supplier.

Students in Years 11 and 12 may continue to use their Chromebook, but if they wish to use an alternative device at school it should have a diagonal screen size of at least 26cm. Requirements are:

- The device must have College supplied Anti-Virus software installed as well as any other software deemed necessary by the College. Students must allow the College to install the required management software on the device. This software must not be deactivated
- A laptop running Windows 10 or 11 (not Windows S) or MacOSMonterey or Ventura
- At least 8GB RAM and 256GB SSD
- At least a Core i5 processor for Windows based laptops
- At least a Core i5 or M1 processor for Mac based laptops

USAGE AND NETWORK ACCESS

While at the College, devices are intended to be used for educational purposes and will access the College network which is monitored and protected by filtering software. The wireless network is secure and access is gained by using an individually allocated Pre-Shared key. To this end, the device must be brought to the College every day with a full battery. There are charging facilities available at the College but students who do not bring a charged device to school may receive a negative (Equipment) notice on their Student Record. Students are only permitted to access the College's network. They are not permitted to use private networks or mobile 'hotspots'.

COMMUNICATION

Whether at the College or at home, students are encouraged to utilise the provided communication facilities to communicate collaboratively or individually with staff and other students. All email communications are recorded and retained for security and accountability purposes. Google Meets, Hangouts, Chats, Classroom activity is also retained. Video conferences via Google or other platforms

such as Zoom may also be retained. For this reason, these formats should only be used for College communication and not personal use.

LOSS, THEFT, DAMAGE AND BACKUP

Data in the email facility (for example attachments to emails) may not be backed up by the College and it is therefore the responsibility of the student to maintain a copy of their work externally from their email account. Any data to be retained should be backed up to Google Drive and / or onto physical media such as USB flash drive or USB hard disk drive.

The College cannot take responsibility for the loss, damage, misuse, or theft of Chromebooks, laptops, tablets or other digital devices including mobile phones and smartwatches while travelling to and from school or at school. Students who bring mobile devices, digital devices, phones/smartwatches to school do so at their own risk. The College accepts no responsibility for investigating or replacing lost, stolen or damaged mobile/digital devices, phones/smartwatches. The student/owner bears full responsibility for the security of the device.

Loss of digital assessment work is not accepted as a valid reason for non-submission or late submission of assessment tasks. Data should be stored on Google drive where possible to minimise the chances of loss. Students may also use an external drive to backup data.

Chromebooks purchased via the portal have a 3 year warranty. The ICT team will act as a go- between for repairs. Breakage is not covered under warranty so parents should consider insurance for the device. The ICT team will endeavour to offer the most cost effective option for repairs where possible. Repair costs are payable in advance.

All digital devices should be able to be clearly identified by their owner. Students who bring a mobile device, digital device, mobile phone to school are advised to store it securely in their locker when not in use. It is strongly advised that students use passwords/pin numbers to ensure that unauthorised access and/or phone calls/messages cannot be made. Students must keep their password/pin numbers confidential. Mobile phones/smartwatches and/or passwords may not be shared.

USAGE AWAY FROM THE COLLEGE

Outside of the College devices may be connected to any home network or internet connection. Limited filtering and security measures are applied through Google 24 hours a day, 7 days a week. This means that activity on the Chromebook, or in fact any device if the user is logged into their @bcc account may be stored in Google Vault where it may be accessed if deemed necessary. Parents/carers should investigate and apply a home network filtering solution. Advice about home network filtering is available from the College ICT team, and will be provided when undertaking the required BCC Digital Discipleship course.

LOAN DEVICES

A short term loan device (ie Chromebook) may be provided by the College if a student does not have a functional Chromebook. A charger may also be provided. The parent of the student is liable for any damage that occurs to these devices while on loan. If the cost of the repair is not paid within two weeks a $40 administration fee is applied.

RESPONSIBLE USE

Students are expected to act responsibly and thoughtfully when using technology resources.

All Internet usage is logged and will be monitored. Any staff member can request a student to immediately exit a website which the staff member decides is inappropriate. Failure to do so will be deemed an offence and lead to possible disciplinary action.

If any user suspects their password has become compromised or that another user has accessed their account, the concern should be reported to the Class Teacher immediately. Devices should only be used as directed by a classroom teacher. During recess and lunch the device should be in the student's locker. Year 11 and 12 students can use their device during recess and lunch, but only in the Library or Year 12 Common Room. Other students may use their laptops or approved device in the library with permission and/or under supervision. The following activities are forbidden and, if detected, will result in loss of access to computers and the network, and possible other disciplinary action. Some offences may incur legal action of a civil or criminal nature.

1. Giving personal log-on or password details to other users
2. Attempting to access or lock another user's account
3. Deliberately damaging computer equipment
4. Deliberately corrupting software
5. Attempting to bypass any network security
6. Sending, displaying or downloading messages, text or graphics which could reasonably be interpreted as threatening, obscene, harassing, pornographic or overtly anti-Christian
7. Accessing banned sites
8. Deliberately corrupting files of self or others
9. Deliberately spreading computer viruses
10. Deliberately recording staff and other student interactions on any device without prior agreement. Recording audio or video media or taking pictures of any student or staff member without their permission
11. Sending, displaying or downloading any material which contravenes existing Commonwealth or Territory laws on racial vilification, sexual harassment, violence and defamation
12. Attempting to access any computer application, such as administrative systems, illegally or without authorization
13. Outright breach of copyright or plagiarism of others' work
14. Using Artificial Intelligence to generate classwork, aside from when specifically prescribed by the class teacher
15. Doing unnecessary or excessive printing
16. Downloading large files from the Internet
17. Using the network for storage of files that are not related to school work
18. Defaming any member of the College community on any digital device or medium
19. Bringing the College name (Belmont Christian College) into disrepute in any form
20. Electronic communications of any means is not to be used by students to communicate with parents if they are being disciplined. It remains the prerogative of the College to inform parents of this as deemed necessary
21. Playing online games during learning activities, which are not relevant to the learning or of the knowledge/permission of the teacher

All activity on @bcc accounts are monitored at all times in all locations. In addition to this, the College reserves the right to inspect, copy and review a personally owned device or file when administration has a reasonable suspicion that a violation has occurred.

Mobile Devices

PURPOSE

The widespread ownership of mobile digital devices requires that school administrators, teachers, students, and parents/carers take steps to ensure that such devices are used responsibly at school. This Acceptable Use Policy is designed to ensure that potential issues involving said devices can be clearly identified and addressed, ensuring the benefits that the devices provide (such as increased safety) can continue to be enjoyed by our students.

BCC has established this Digital Devices Acceptable Use Policy to provide teachers, students and parents/carers guidelines and instructions for the appropriate use of mobile devices during school hours.

Students, their parents/carers should read and understand the Acceptable Use Policy before students are given permission to bring mobile devices to school. The Acceptable Use Policy also applies to students during school excursions, camps and extra-curricular activities if such devices have been permitted.

ACKNOWLEDGEMENT

Personal safety and security: BCC accepts that parents/carers give their children mobile phones/smartwatches to protect them from everyday risks involving personal security and safety. There is also increasing concern about children travelling alone on public transport or commuting long distances to school. It is acknowledged providing a child with such devices gives parents/carers reassurance that they can contact their child if they need to speak to them urgently.

RESPONSIBILITY

Students bring their mobile devices, digital devices, phones/smartwatches to school at their own risk. The College is not responsible for mobile devices, digital devices, phones/smartwatches that are lost, stolen or damaged at school or when students are travelling to and from school. It is the responsibility of students who bring such devices to school to abide by the guidelines outlined in this document.

The decision to provide a mobile device, digital device, phone/smartwatch to their children should be made by parents/carers if they deem it necessary. Parents/carers should be aware if their child takes a mobile device, digital device, mobile phone/smartwatch to school.

Permission to have a mobile device, digital device, mobile phone/smartwatch at school and/or while under the school's supervision is contingent on parent/carers permission in compliance with this policy. Parents/carers may revoke approval at any time.

ACCEPTABLE USE

While onsite, including lesson times, mobile devices are to remain out of plain view. Smartwatches should be turned off mobile device mode if possible. During class time, if the mobile devices are to be used, they may only be used under teacher direction. Mobile devices should not be used when a student leaves the classroom to access change-rooms, toilets or to go to the Office, etc....

During recess and lunch, mobile devices should not be used and be kept out of sight, locked away in lockers, switched off or switched to soundless features. Allowances may be permitted only in exceptional circumstances if the parent/carers specifically requests it in writing (or as in 4.5 below). Such requests will be handled on a case-by-case basis and should be directed to the Heads of School. Parents/carers are reminded that in cases of emergency, the College office remains the appropriate point of contact and can ensure your child is reached quickly and assisted in an appropriate way.

Smart watches will be permitted to be used in a similar manner to analogue watches. Inappropriate use of smartwatches (such as accessing functions available on mobile phones) may result in similar action being taken for the unacceptable use of mobile devices.

Mobile devices, digital devices, phones/smartwatches should not be used in any manner or place that is disruptive to the normal routine of the school.

Students requiring the use of their mobile device for medical purposes or as part of their IP will be permitted access. This will be managed by the Learning Enrichment Coordinator and Wellbeing (Secondary School) and Class Teachers and Stage Leaders (Primary School). If a student must take or make a call, send or receive a message, they must ask the permission of a teacher (or office staff) who will use discretion in their decision and, if granted, monitor the call.

Students should protect their phone numbers by only giving it to friends and knowing who they have given it to. This can help protect the student's number being used by others and may guard against the receipt of insulting, threatening or unpleasant voice, text and picture messages.

UNACCEPTABLE USE

Unless express permission is granted by staff, mobile devices, digital devices, phones/smartwatches should not be used to make calls, send SMS messages, access the internet, record/take photos/videos, access social media, check the time or any other application during school lessons and other educational activities, such as assemblies, excursions, etc....

Mobile devices, digital devices, phones/smartwatches must not disrupt classroom lessons with alerts, ringtones or beeping. Should there be repeated disruptions to lessons caused by a mobile device, digital device, phone/smartwatch, the responsible student may face disciplinary actions by the Heads of School as sanctioned by the Principal.

Using mobile devices/digital devices to participate in cyberbullying, including sharing inappropriate content or abuse transmitted electronically such as by email, Social Media, SMS text messages or apps such as Snapchat, Instagram or by other electronic means. Any such action will be dealt with according to the College Discipline Policy and Procedures. Please note that it is a criminal offence to use a mobile device to menace, harass or offend another person. As such, if action as sanctioned by the Principal is deemed ineffective, as with all such incidents, the College may consider it appropriate to involve the police.

Mobile devices, digital devices, phones/smartwatches are not to be used or taken into private areas such as change rooms or toilets, or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.

Mobile devices, digital devices, phones/smartwatches are not to be used by students to bypass College procedures in relation to school - parent/carer contact. Any messages for students are managed through the College Office. If a student needs to contact a parent/carer during lesson time, this is to be managed through the College Office.

Any student/s caught using a mobile device, phone/smartwatch to cheat in exams or assessments will face disciplinary actions by the Heads of School as sanctioned by the Principal.

CONSEQUENCES

Students who infringe the rules set out in this agreement could face having their mobile devices, digital devices, phones/smartwatches confiscated as outlined below, or permission to bring a mobile device, digital device, phone/smartwatch to the College withdrawn.

On the first occasion of a teacher seeing or hearing a mobile device, digital device, phone/smartwatch or detecting that it is being used secretively or evidence shows that the mobile device, digital device, phone/smartwatch has been used without permission, the student will be required to hand the mobile device, digital device, phone/smartwatch to staff who in turn will give it to the College Office staff for recording and storage until the end of the school day when the student may come to the office and request its return. This will be done with a warning of the consequences as outlined below.

On the second confiscation, a parent/carer of the student will be required to come to the College to collect the mobile device, digital device, phone/smartwatch and the student will be placed on a Head of School detention (Secondary School), or Talk and Sort (Primary School). The parent/carer will be informed that if there is a third confiscation, the student will be placed on a Tuesday After-School Detention (Secondary) or Talk & Sort (Primary) and the mobile device, digital device, phone/smartwatch held by the Heads of School until the end of the current school term.

Any subsequent confiscation that year will result in a suspension (up to 3 days) and the withdrawal of permission for the student to bring a mobile device, digital device, phone/smartwatch to the College for the remainder of the current year.

If a student refuses to hand a mobile device, digital device, phone/smartwatch to a staff member who is confiscating the device, they will be suspended until the device is surrendered and/or possibly be placed on Head of School detention (Secondary School), or Talk and Sort (Primary School), and permission for the student to bring a mobile device, digital device, phone/smartwatch to the College may be withdrawn.

Mobile devices, digital devices, phones/smartwatches confiscated due to misuse will be held at the College and appropriate discipline, including possible suspension, administered at the discretion of the Heads of School as sanctioned by the Principal.

As per the section above, failure to heed the rules set out in this document may result in an alleged incident being referred to the police for investigation. In such cases, the parent/carer would be notified immediately.

For further information about the safe, responsible use of digital devices, rights and accountability please consult:

- The eSafety Commissioner
- NSW Government Education Legal Issues Bulletin 35 - Misuse of Technology in Schools

Digital Device Responsible Use Summary

I understand that I am encouraged to read the full Digital Devices Acceptable Usage Policy available on the College website or from the College Office.

I understand that I must have completed the College's Digital Discipleship course before I am given access to the College's network.

I understand that that this agreement will be kept on file at the College and the details may be used (and shared with a third party if necessary) to assist in identifying a mobile device/ digital device including a phone and/or smartwatch should the need arise (e.g. if the College determines that the mobile device, phone/smartwatch is being used inappropriately).

The following conditions will help you become a responsible Digital Citizen.

1. **Respect Yourself:** I will show respect for myself through my actions. I will select online names that are appropriate, I will consider the information and images that I post online. I will consider what personal information about my life, experiences, experimentation or relationships I post. I will not be obscene.
2. **Protect Yourself:** I will ensure that the information, images and materials I post online will not put me at risk. I will not publish my personal details, contact details or a schedule of my activities. I will report any attacks or inappropriate behaviour directed at me. I will protect passwords, accounts and resources.
3. **Respect Others:** I will show respect to others. I will not use electronic mediums to defame, bully, harass or stalk other people. I will show respect for other people in my choice of websites, I will not visit sites that are degrading, pornographic, racist or inappropriate. I will not abuse my rights of access and I will not enter other people's private spaces or areas. I will respect other student's property.
4. **Protect Others:** I will protect others by reporting abuse, not forwarding inappropriate materials or communications; and not visiting sites that are degrading, pornographic, racist or inappropriate.
5. **Respect Intellectual Property:** I will request permission to use resources. I will suitably cite any and all use of websites, books, media etc. I will validate information. I will use and abide by the fair use rules.
6. **Protect Intellectual Property:** I will request to use the software and media others produce. I will use free and open source alternatives rather than pirating software. I will purchase, license and register all software. I will purchase my music and media, and refrain from distributing these in a manner that violates their licenses. I will act with integrity.
7. **Respect College Online Rules:** I will only use the College network as directed by my teacher during school hours. I will not access Social Media while onsite at the College.
8. **Mobile phone/device:** I will only use my mobile phone/device onsite with permission and under supervision of College staff.
9. **Continuity of learning:** My devices will not interrupt others and my learning or school based activities. This means notifications will remain silenced and I will not check Social Media, in class, between classes or during breaks or on school based activities.
10. **Respect Privacy:** I will not use devices in private spaces, such as leaving the classroom and going to the bathroom, playground or the College Office.
11. **Artificial Intelligence**: I will not use artificial intelligence to generate classwork, aside from when specifically prescribed by the class teacher.
12. **Respecting Learning**: I will not play online games during learning activities, which are not relevant to the learning or of the knowledge/permission of the teacher.